

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN**

AUTHENTICOM, INC.

Plaintiff,

Case No. 17-cv-318

vs.

Redacted Version

CDK GLOBAL, LLC; and THE REYNOLDS
AND REYNOLDS COMPANY

Defendants.

**AUTHENTICOM'S REPLY
IN SUPPORT OF ITS MOTION FOR A PRELIMINARY INJUNCTION**

TABLE OF CONTENTS

	Page
TABLE OF AUTHORITIES	iii
INTRODUCTION	1
I. The Equities Strongly Favor Preliminary Injunctive Relief	4
A. Defendants’ Opposition Confirms That Authenticom Will Suffer Irreparable Harm in the Absence of a Preliminary Injunction	4
1. Defendants Admit That, Absent an Injunction, They Will Cut Off Authenticom From Serving Dealers, Putting Authenticom Out of Business	4
2. Defendants Do Not Dispute That Authenticom Is Suffering Irreparable Loss of Customer Goodwill.....	5
3. Defendants’ Denials of Irreparable Harm Are Unpersuasive	6
B. The Balance of Harms Favors Relief.....	9
1. The Existential Threat Posed To Authenticom Weighs Heavily In Favor of Relief.....	9
2. Defendants’ Speculative Claims Cannot Tip the Balance of Harms	10
a. There Is No Evidence That Authenticom’s Access Causes DMS Disruptions	10
b. Defendants Have No Evidence That Authenticom’s Data Access Compromises Data Security	13
c. Claim of Harm To Investment Incentives Is Implausible And Unsubstantiated	18
C. Granting Relief Is in the Public Interest	20
1. Absent an Injunction, Dealers, Vendors, and Car Buyers Will Suffer Higher Prices.....	20
2. The Jobs and Livelihoods of Authenticom’s Employees Further Support Preliminary Injunctive Relief.....	20
3. Authenticom’s Business Model Is Legal	21
D. The Injunction Sought Is Not a Mandatory Injunction And Satisfies Rule 65.....	22
II. Authenticom Has Shown a Strong Likelihood of Success on the Merits	24

A. Authenticom’s Section 1 Claims Based on Horizontal Agreement Are Legally
Unchallenged and Factually Supported 24

1. Defendants’ Agreement To Block Authenticom Is Unlawful Per Se And
Strongly Supported By the Evidence 24

2. Defendants’ Market Division Agreement Is Also Unlawful Per Se 28

B. Authenticom Is Likely To Succeed on Its Tying Claim 30

C. Authenticom Is Likely To Succeed on Its Claims Under the Rule of Reason..... 32

D. Authenticom Is Likely To Succeed On Its Section 2 After-Market Claims 34

E. Because the Restrictions on Dealing with Independent Integrators Are
Unlawful, Defendants’ Conduct Is Not Privileged, and Authenticom’s Tortious
Interference Claim Is Likely To Succeed 39

III. No Bond Is Warranted 39

CONCLUSION..... 41

TABLE OF AUTHORITIES

	Page
CASES	
<i>A Woman’s Choice-East Women’s Clinic v. Newman</i> , 904 F. Supp. 1434 (S.D. Ind. 1995)	9
<i>American Needle, Inc. v. National Football League</i> , 560 U.S. 183 (2010).....	29
<i>Andrx Pharm., Inc. v. Biovail Corp. Int’l</i> , 256 F.3d 799 (D.C. Cir. 2001).....	29
<i>Arc of California v. Douglas</i> , 757 F.3d 975 (9th Cir. 2014).....	7
<i>Arizona v. Maricopa Cty. Med. Soc’y</i> , 457 U.S. 332 (1982)	32
<i>Assessment Techs. Of WI, LLC v. WIREdata, Inc.</i> , 350 F.3d 640 (7th Cir. 2003).....	19
<i>Avaya Inc. v. Telecom Labs, Inc.</i> , 2014 WL 2940455 (D. N.J. June 30, 2014).....	37
<i>Batson v. Live Nation Entm’t, Inc.</i> , 746 F.3d 827 (7th Cir. 2014).....	31
<i>Boardman v. Pacific Seafood Grp.</i> , 822 F.3d 1011 (9th Cir. 2016)	20
<i>Briesemeister v. Lehner</i> , 720 N.W.2d 531 (Wis. Ct. App. 2006)	38
<i>Burda v. Wendy’s Int’l, Inc.</i> , 659 F. Supp. 2d 928 (S.D. Ohio 2009).....	37
<i>C & N Corp. v. Kane</i> , 142 F. Supp. 3d 783 (E.D. Wis. 2015).....	23
<i>Carlson Grp., Inc. v. Davenport</i> , 2016 WL 7212522 (N.D. Ill. Dec. 13, 2016).....	7
<i>Carrillo v. Schneider Logistics, Inc.</i> , 823 F. Supp. 2d 1040 (C.D. Cal. 2011).....	39, 40
<i>Checker Car Club of Am., Inc. v. Fay</i> , 2017 WL 1079251 (N.D. Ill. Mar. 22, 2017).....	7
<i>Collins Inkjet Corp. v. Eastman Kodak Co.</i> , 781 F.3d 264 (6th Cir. 2015).....	20
<i>Concerned Pastors for Social Action v. Khouri</i> , 220 F. Supp. 3d 823 (E.D. Mich. 2016).....	39
<i>Craigslist Inc. v. 3Taps Inc.</i> , 964 F. Supp. 2d 1178 (N.D. Cal. 2013).....	22
<i>Datel Holdings Ltd. v. Microsoft Corp.</i> , 712 F. Supp. 2d 974 (N.D. Cal. 2010).....	34, 36
<i>Dos Santos v. Columbus-Cuneo-Cabrini Med. Ctr.</i> , 684 F.2d 1346 (7th Cir. 1982)	30
<i>EF Cultural Travel BV v. Explorica, Inc.</i> , 274 F.3d 577 (1st Cir. 2001)	21

<i>Eastman Kodak Co. v. Image Tech. Servs.</i> , 504 U.S. 451 (1992)	35, 36, 37
<i>Essentia Health v. Gundersen Lutheran Health Sys., Inc.</i> , 2017 WL 1318112 (W.D. Wis. Apr. 7, 2017)	7
<i>Ezell v. City of Chicago</i> , 651 F.3d 684 (7th Cir. 2011)	10
<i>First Union Nat’l Bank v. Burke</i> , 48 F. Supp. 2d 132 (D. Conn. 1999)	22
<i>Garcia v. Google, Inc.</i> , 786 F.3d 733 (9th Cir. 2015)	22
<i>Gateway E. Ry. Co. v. Terminal R.R. Ass’n of St. Louis</i> , 35 F.3d 1134 (7th Cir. 1994).....	5
<i>General Leaseways, Inc. v. National Truck Leasing Ass’n</i> , 744 F.2d 588 (7th Cir. 1984)	28
<i>Girl Scouts of Manitou Council, Inc. v. Girl Scouts of U.S. of Am., Inc.</i> , 549 F.3d 1079 (7th Cir. 2008).....	4
<i>Gumwood HP Shopping Partners, L.P. v. Simon Prop. Grp., Inc.</i> , 2016 WL 6091244 (N.D. Ind. Oct. 19, 2016)	31, 34
<i>Gutierrez v. City of East Chicago</i> , 2016 WL 5819818 (N.D. Ind. Sept. 6, 2016).....	39
<i>High Fructose Corn Syrup Antitrust Litig., In re</i> , 295 F.3d 651 (7th Cir. 2002)	26
<i>Hoosier Energy Rural Elec. Coop., Inc. v. John Hancock Life Ins. Co.</i> , 582 F.3d 721 (7th Cir. 2009)	8
<i>Hugler v. Valley Garlic, Inc.</i> , 2017 WL 2021531 (E.D. Cal. May 12, 2017).....	8
<i>Ideal Indus., Inc. v. Gardner Bender, Inc.</i> , 612 F.2d 1018 (7th Cir. 1979)	7
<i>International Airport Ctrs. L.L.C. v. Citrin</i> , 440 F.3d 418 (7th Cir. 2006)	21
<i>Jacobson & Co. v Armstrong Cork Co.</i> , 548 F.2d 438 (2d Cir. 1977)	22
<i>Jefferson Par. Hosp. Dist. No. 2 v. Hyde</i> , 466 U.S. 2 (1984), <i>abrogated on other grounds by Illinois Tool Works Inc. v. Independent Ink, Inc.</i> , 547 U.S. 28 (2006)	31
<i>Klor’s, Inc. v. Broadway-Hale Stores, Inc.</i> , 359 U.S. 207 (1959)	26
<i>LVRC Holdings LLC v. Brekka</i> , 581 F.3d 1127 (9th Cir. 2009).....	21
<i>Legal Aid Soc’y of Haw. v. Legal Servs. Corp.</i> , 961 F. Supp. 1402 (D. Haw. 1997)	22

<i>MB Fin. Bank, N.A. v. MB Real Estate Servs., L.L.C.</i> , 2003 WL 21462501 (N.D. Ill. June 23, 2003).....	7
<i>M.R. v. Dreyfus</i> , 697 F.3d 706 (9th Cir. 2012)	8
<i>Monster Energy Co. v. Wensheng</i> , 136 F. Supp. 3d 897 (N.D. Ill. 2015)	39
<i>Morton Grove Pharm., Inc. v. Par Pharm. Cos.</i> , 2006 WL 850873 (N.D. Ill. Mar. 28, 2006)	35
<i>Nano-Proprietary, Inc. v. Keesmann</i> , 2007 WL 433100 (N.D. Ill. Jan. 30, 2007).....	10
<i>National Soc’y of Prof’l Eng’rs v. United States</i> , 435 U.S. 679 (1978)	25
<i>Navajo Health Found.-Sage Mem’l Hosp., Inc. v. Burwell</i> , 100 F. Supp. 3d 1122 (D. N.M. 2015).....	40-41
<i>North Alamo Water Supply Corp. v. City of San Juan, Tex.</i> , 90 F.3d 910 (5th Cir. 1996).....	23
<i>Northern Star Indus., Inc. v. Douglas Dynamics LLC</i> , 848 F. Supp. 2d 934 (E.D. Wis. 2012)	7
<i>PSI Repair Servs., Inc. v. Honeywell, Inc.</i> , 104 F.3d 811 (6th Cir. 1997)	36
<i>Perfect 10, Inc. v. Google, Inc.</i> , 653 F.3d 976 (9th Cir. 2011)	9
<i>Premier Elec. Const. Co. v. Nat’l Elec. Contractors Ass’n, Inc.</i> , 814 F.2d 358 (7th Cir. 1987)	29
<i>Red Lion Medical Safety, Inc. v. Ohmeda, Inc.</i> , 63 F. Supp. 2d 1218 (E.D. Cal. 1999).....	35
<i>Reinders Bros., Inc. v. Rain Bird E. Sales Corp.</i> , 627 F.2d 44 (7th Cir. 1980)	6
<i>Russian Media Group, LLC v. Cable Am., Inc.</i> , 598 F.3d 302 (7th Cir. 2010)	23
<i>SMC Corp. v. Lockjaw, LLC.</i> , 481 F. Supp. 2d 918 (N.D. Ill. 2007)	6
<i>Saad v. Village of Orland Park</i> , 2011 WL 6754042 (N.D. Ill. Dec. 23, 2011)	23
<i>SanDisk Corp. v. Kingston Tech. Co.</i> , 863 F. Supp. 2d 815 (W.D. Wis. 2012)	34
<i>Stokely-Van Camp, Inc. v. Coca-Cola Co.</i> , 1987 WL 6300 (N.D. Ill. Jan. 30, 1987)	7
<i>Stone v. City and County of San Francisco</i> , 145 F.R.D. 553 (N.D. Cal. 1993).....	22
<i>Texas Children’s Hosp. v. Burwell</i> , 76 F. Supp. 3d 224 (D.D.C. 2014).....	7

<i>Tom Doherty Assocs., Inc. v. Saban Entm’t, Inc.</i> , 60 F.3d 27 (2d Cir. 1995).....	7
<i>Toys “R” Us, Inc. v. FTC</i> , 221 F.3d 928 (7th Cir. 2000)	24
<i>United States v. Apple, Inc.</i> , 791 F.3d 290 (2d Cir. 2015).....	29
<i>United States v. Mercedes-Benz of N. Am., Inc.</i> , 517 F. Supp. 1369 (N.D. Cal. 1981)	29
<i>United States v. Microsoft Corp.</i> , 253 F.3d 34 (D.C. Cir. 2001)	34
<i>Verizon Commc’ns Inc. v. Law Offices of Curtis V. Trinko, LLP</i> , 540 U.S. 398 (2004)	37
<i>Washington State Apple Advert. Comm’n, In re</i> , 257 F. Supp. 2d 1274 (E.D. Wash. 2003)	40
<i>Wayne Chem., Inc. v. Columbus Agency Serv. Corp.</i> , 567 F.2d 692 (7th Cir. 1977)	39
<i>ZF Meritor, LLC v. Eaton Corp.</i> , 696 F.3d 254 (3d Cir. 2012).....	37

STATUTES AND RULES

18 U.S.C. § 1030(a)(2)(c)	21
Fed. R. Civ. P. 65	22
Fed. R. Civ. P. 65(c)	38

OTHER MATERIALS

Restatement (Second) of Torts.....	38
------------------------------------	----

INTRODUCTION

Defendants make no bones about their intentions: they want to put Authenticom out of business. If Defendants' conduct is not enjoined promptly, Authenticom will be shut out from at least 72 percent of all dealers in the country (i.e., those that use CDK's or Reynolds' DMS platform). If it is foreclosed from such a large portion of the market, Authenticom's celebrated success story will come to a shattering end, and 120 Wisconsin residents will lose their jobs.

Calling Authenticom's business model "hostile" and "illegal," Defendants defend their efforts to exclude Authenticom from competing to provide vendors and dealers the integration services that they require. But Defendants do not and cannot defend a horizontal *agreement* to block third-party integrators: no supposed concerns about security could justify conspiring with a direct competitor to exclude a rival. *See* Defs. Opp. at 30 (Dkt. 105) ("Defs. Opp.") (offering only "economic reasons for defendants' *independent* decisions to 'close' their DMSs") (emphasis added). And the evidence of that agreement – which Defendants' own employees bragged about – has only grown stronger: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Moreover, Defendants efforts to explain away their written agreement not to compete in the market for integration services hold no water: CDK had been competing to provide integration services for dealers using the Reynolds DMS until it agreed with Reynolds to stop. And the agreement is worse than originally thought: the

[REDACTED]

[REDACTED] Given the undisputed, *per se* illegality of the horizontal agreement between the two dominant DMS

providers, and the ample evidence of such an agreement, Authenticom's likelihood of success on the merits is strong indeed.

Moreover, in addition to the compelling evidence of an unlawful horizontal agreement, the evidence of anticompetitive effects from Defendants' unlawful vertical arrangements – massive price increases for integration services that are not offset by any proven benefit – stands essentially un rebutted. Such a showing also satisfies Plaintiffs' burden at this pre-discovery stage. And, as for Defendants' purported efficiency justifications, Defendants' own documents belie their supposed concerns over “security” and “system integrity.” [REDACTED]

[REDACTED]

see also Fitkin Supp. Decl. ¶¶ 9-11.

The balance of harms weighs heavily in favor of preserving the status quo rather than allowing Defendants to carry out their concerted plan to extinguish Authenticom. [REDACTED]

[REDACTED]

[REDACTED] Before then, Reynolds only tepidly enforced its contracts starting in 2009 and CDK did not do so at all. In the meantime, competition to provide integration services flourished, with *CDK itself* as one of the most vigorous competitors and with Reynolds (for its own applications) as one of the most avid consumers of independent integrators' services, including Authenticom's. Having affirmatively fostered and participated in this market for decades, Defendants cannot now credibly claim that a modest injunction

temporarily maintaining the status quo pending the resolution of this litigation would cause them any cognizable harm.

The public interest also supports a preliminary injunction. Consumers – antitrust law’s reason for being – support Authenticom. Defendants, despite contracts with the vast majority of U.S. car dealers, could muster but a single lukewarm declaration from one dealer to bolster their case. In contrast, dealers and vendors across the country have lined up behind Authenticom to oppose Defendants’ anticompetitive practices. Vendors and dealers know that, if left unchecked, Defendants’ exclusionary efforts will deprive them of the only competitive force that constrains Defendants’ ability to charge sky-high prices for data integration on top of the sky-high prices that they already charge for DMS services. Once Authenticom is gone, the consequence will be even higher prices for vendors and dealers. Compared to these widespread and foreseeable harms, which are grounded in basic economic principles, Defendants’ speculative suggestion that access by Authenticom – which has not suffered a single cyber security event in its history – might facilitate a cyberattack on Defendants’ DMS systems does not pass muster.

The Court should grant Authenticom’s motion and temporarily enjoin CDK and Reynolds from disabling dealer-created login credentials, from enforcing contractual provisions that prevent dealers and vendors from doing business with Authenticom, and from retaliating against dealers and vendors that choose to deal with Authenticom.

I. THE EQUITIES STRONGLY FAVOR PRELIMINARY INJUNCTIVE RELIEF

A. Defendants' Opposition Confirms That Authenticom Will Suffer Irreparable Harm in the Absence of a Preliminary Injunction

1. Defendants Admit That, Absent an Injunction, They Will Cut Off Authenticom From Serving Dealers, Putting Authenticom Out of Business

Defendants' brief makes one thing clear: they are actively blocking Authenticom's dealer-authorized access to dealer data stored on DMS databases and will continue to do so if no injunction is granted.¹ CDK and Reynolds have made no secret that they are trying to destroy Authenticom's business. Their brief openly acknowledges this. *See, e.g.*, Defs. Opp. at 3 (stating that Defendants "design[ed] their respective systems to prevent hostile third-party data extractors like Authenticom from accessing them"); *id.* at 12 (describing Reynolds' effort "to protect its DMS from unauthorized third party access – . . . like Authenticom's"); *id.* at 15 ("The centerpiece of [CDK's] SecurityFirst initiative was to move DMS access away from hostile third-parties like Authenticom."). Defendants have repeatedly stated their intent to destroy Authenticom's business and are actively attempting to do so.²

¹ *See, e.g.*, [REDACTED] Fitkin Supp. Decl. ¶¶ 17-20 (explaining that CDK recently implemented heightened blocking measures against Walter's Automotive Group in retaliation for its participation in this suit).

² [REDACTED]

If CDK and Reynolds succeed in completely foreclosing Authenticom from serving 72 percent of dealerships nationwide (Defendants' acknowledged combined market share),³

Authenticom will [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Granting the injunction, by contrast, will allow Authenticom to maintain if not expand its existing customer and revenue base until it has an opportunity to prove its case at trial.

In short, Defendants' own submissions show that this is precisely the type of case for which injunctive relief is warranted: to preserve Authenticom as an ongoing concern so that it has a chance to prove its case on the merits. *See Girl Scouts of Manitou Council, Inc. v. Girl Scouts of U.S. of Am., Inc.*, 549 F.3d 1079, 1095 (7th Cir. 2008).

2. Defendants Do Not Dispute That Authenticom Is Suffering Irreparable Loss of Customer Goodwill

Defendants also have no response to Authenticom's evidence that their conduct is causing Authenticom to suffer irreparable loss of goodwill. Neither Defendants nor their expert, Professor Zmijewski, attempt to rebut Authenticom's evidence that numerous vendors and

[REDACTED]

³After Authenticom filed its initial motion, CDK announced it is acquiring the nation's fourth-largest DMS provider, Auto/Mate – which services 1,200 dealerships (or 7 percent of the market). *See* Pl. Reply in Support of SOF ¶ 5. If that transaction is completed, Defendants would control nearly 80 percent of the DMS market.

dealers have stopped working with Authenticom as a result of Defendants' disruptions to Authenticom's ability to provide reliable data integration services. *See, e.g.*, SOF ¶¶ 231-234 (Dkt. 63) ("SOF"). Nor do they dispute that Authenticom's ability to serve its remaining customers has been severely compromised by Defendants' blocking. *See id.* ¶ 232. Far from disputing these points, Defendants admit they are actively harming Authenticom's relationships with its customers by trying to cut Authenticom off from accessing their DMS systems on behalf of dealers. Authenticom's "loss of goodwill . . . qualifies as irreparable harm for which there is no adequate remedy at law." *See Gateway E. Ry. Co. v. Terminal R.R. Ass'n of St. Louis*, 35 F.3d 1134, 1140 (7th Cir. 1994); *see also SMC Corp. v. Lockjaw, LLC.*, 481 F. Supp. 2d 918, 927-28 (N.D. Ill. 2007) ("loss of customers" constitutes irreparable harm) (collecting cases); *Reinders Bros., Inc. v. Rain Bird E. Sales Corp.*, 627 F.2d 44, 53 (7th Cir. 1980) (loss of portion of clientele built during 20 years in business constitutes irreparable harm).

3. Defendants' Denials of Irreparable Harm Are Unpersuasive

Defendants' responses to Authenticom's irreparable harm arguments are unconvincing.

First, Defendants argue (at 49-50) that Authenticom's claim of irreparable harm is implausible because Authenticom allegedly delayed in bringing this lawsuit and motion. Defendants' cry of undue delay is the same argument they made in moving to summarily dismiss Authenticom's motion (Dkt. 74). This Court declined to accept that argument then, and it should not accept it now. As it previously explained (Dkt. 80), Authenticom tried to endure Defendants' anticompetitive conduct by working with customers to mitigate Defendants' blocking efforts. It also tried to work with its banks to refinance its debt obligations. But litigation became an unfortunate necessity shortly after [REDACTED]

[REDACTED]

Furthermore, any delay would not undermine Authenticom’s irreparable harm showing. “[M]ere evidence of delay without any explanation on [defendant’s] part of why such a delay negatively affected it, would not lessen [plaintiff]’s claim of irreparable injury.” *Northern Star Indus., Inc. v. Douglas Dynamics LLC*, 848 F. Supp. 2d 934, 950 (E.D. Wis. 2012); *see also*

⁴ See also *Tom Doherty Assocs., Inc. v. Saban Entm't, Inc.*, 60 F.3d 27, 39 (2d Cir. 1995) (“parties should not be encouraged to sue before a practical need to do so has been clearly demonstrated.”); *Texas Children’s Hosp. v. Burwell*, 76 F. Supp. 3d 224, 244-45 (D.D.C. 2014) (rejecting argument that plaintiff’s three-year delay in filing suit undercut its claim for irreparable harm where the plaintiff “reasonably pursued non-litigation avenues first”).

⁵ The cases Defendants cite (at 50) are factually inapposite. *See Essentia Health v. Gundersen Lutheran Health Sys., Inc.*, 2017 WL 1318112, at *8 (W.D. Wis. Apr. 7, 2017) (finding no irreparable harm because plaintiff’s “theory of irreparable harm is unclear and undeveloped,” and noting that “there is no general rule that plaintiff is barred from seeking an injunction” because of delay; rather, delay is a factor the court can “consider”); *Carlson Grp., Inc. v. Davenport*, 2016 WL 7212522, at *7 (N.D. Ill. Dec. 13, 2016) (finding no irreparable harm not because of any delay, but because there was evidence that money damages were available and plaintiff could not specify what business or contracts would be lost). The remaining cases apply a different standard under trademark law for assessing irreparable harm. *See Checker Car Club of Am., Inc. v. Fay*, 2017 WL 1079251, at *5 (N.D. Ill. Mar. 22, 2017) (presumption of irreparable harm as a result of trademark infringement is “negated where the plaintiff has delayed in enforcing its rights”); *MB Fin. Bank, N.A. v. MB Real Estate Servs., L.L.C.*, 2003 WL 21462501, at *20 (N.D. Ill. June 23, 2003) (trademark infringement case in which court found that there was no irreparable harm due to delay in this specific context); *Stokely-Van Camp, Inc. v. Coca-Cola Co.*, 1987 WL 6300, at *2 (N.D. Ill. Jan. 30, 1987) (same)

Ideal Indus., Inc. v. Gardner Bender, Inc., 612 F.2d 1018, 1025 (7th Cir. 1979) (affirming grant of injunction despite delay of more than four years). Defendants have adduced no evidence of prejudice, and their arguments thus cannot override the imminent, irreparable harm Authenticom and its employees will suffer if Defendants are allowed to put the company out of business before it gets its day in court.

Second, Defendants argue (at 50-51) that Authenticom's financial difficulties are of its own making. However, as Authenticom's expert, Gordon Klein, explains in his reply declaration, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Moreover, there is additional evidence that Authenticom's finances were sound in April 2014, less than a year before Defendants entered into their February 2015 market division agreement. [REDACTED]

[REDACTED]

[REDACTED].

Third, Defendants argue (at 51) that an injunction will not redress Authenticom's irreparable harm. But the evidence demonstrates a direct causal connection between Defendants' efforts to block Authenticom and Authenticom's loss of revenue and customers. Authenticom had experienced steady growth until February 2015, when Defendants entered into their written market division agreement. After that, Authenticom's [REDACTED]

[REDACTED] A "plaintiff

who seeks preliminary injunctive relief must show that irreparable injury is likely in the absence of an injunction,” and “need not further show that the action sought to be enjoined is the exclusive cause of the injury.” *M.R. v. Dreyfus*, 697 F.3d 706, 728 (9th Cir. 2012). Here, Authenticom has demonstrated a “‘sufficient causal connection’ between the alleged injury and the conduct the plaintiff seeks to enjoin such that the injunction would effectively minimize the risk of injury.” *Hugler v. Valley Garlic, Inc.*, 2017 WL 2021531, at *2 (E.D. Cal. May 12, 2017) (quoting *Perfect 10, Inc. v. Google, Inc.*, 653 F.3d 976, 982 (9th Cir. 2011)).

B. The Balance of Harms Favors Relief

1. The Existential Threat Posed To Authenticom Weighs Heavily In Favor of Relief

Under the balance-of-harms sliding scale, the threat to Authenticom’s existence as an ongoing concern weighs heavily in favor of preliminary injunctive relief. *Hoosier Energy Rural Elec. Coop., Inc. v. John Hancock Life Ins. Co.*, 582 F.3d 721, 725 (7th Cir. 2009) (“[T]he more net harm an injunction can prevent, the weaker the plaintiff’s claim on the merits can be while still supporting some preliminary relief.”). Not only is Authenticom’s antitrust case strong on the merits, but the harm an injunction would forestall is enormous: the bankruptcy of the last significant independent data integrator in the market. If Authenticom fails, Defendants will reap the benefits of their anticompetitive campaign, regardless of how Authenticom’s claims are ultimately resolved. This case thus epitomizes the appropriate use of preliminary injunctive relief to preserve the status quo and Authenticom’s right to a meaningful day in court. *See, e.g., A Woman’s Choice-East Women’s Clinic v. Newman*, 904 F. Supp. 1434, 1443 (S.D. Ind. 1995) (“Preliminary injunctions are designed . . . ‘to preserve the court’s power to render a meaningful decision after a trial on the merits.’”) (quoting 11A Wright, Miller & Kane, Fed. Prac. & Proc. 2d, § 2947).

2. Defendants' Speculative Claims Cannot Tip the Balance of Harms

The purported hardships Defendants will face if a preliminary injunction is issued are wholly speculative and, even if credited, pale in comparison to the harm Authenticom will suffer if it is forced to declare bankruptcy and potentially lay off more than 120 employees. *See Ezell v. City of Chicago*, 651 F.3d 684, 710 (7th Cir. 2011) (balance of harms favors the plaintiff where “the harms invoked by the [defendant] are entirely speculative”); *Nano-Proprietary, Inc. v. Keesmann*, 2007 WL 433100, at *7 (N.D. Ill. Jan. 30, 2007) (ignoring “purely speculative” assertions about whether an injunction was in the public interest).

a. There Is No Evidence That Authenticom's Access Causes DMS Disruptions

Defendants contend (at 53) that “third-party access would cause serious disruptions to both DMSs.” But Defendants offer no evidence, apart from conclusory assertions, that Authenticom's data integration services have caused a single disruption of either DMS. Reynolds asserts that its systems are “not designed to support” high volumes of automated queries like Authenticom's. But Reynolds cannot identify even a single instance where Authenticom's automated queries caused a service disruption or other technical problem. CDK's evidence is even weaker, because until 2015, CDK allowed dealers to use third-party data integrators, without any evidence of adverse effects on its systems.⁶

In fact, Authenticom's access causes no technical problems for the DMS because using dealer-provided credentials to pull data does not affect the DMS software. Authenticom simply automates the same report-generating functions that a dealership employee can perform

⁶ CDK claims (at 53) that it provided “active [technological] support” for such access, and that it no longer does so, but (taking that claim at face value) it offers no reason why it cannot provide whatever “support” is needed to avoid disruptions if the injunction is granted.

manually. *See* Cottrell Reply Decl. ¶ 41; Cottrell Decl. ¶ 52. Far from overburdening the DMS, Authenticom’s queries complete in mere minutes. *See* Cottrell Reply Decl. ¶¶ 36-37, 40. And Authenticom schedules the vast majority of its queries to run overnight, during non-business hours, to ensure that these already light queries cannot affect dealers’ operations. *See id.* ¶¶ 36, 39. Overnight queries result in the transfer of approximately 5 MB of data – roughly the same size as a photograph taken with a smart phone. *See id.* ¶ 36; *see also* Swire Reply Decl. ¶ 68. The queries that are run during the day for approximately 100 of Authenticom’s 11,000 dealership customers likewise take a matter of minutes and result in the transfer of roughly 1 MB of data. *See* Cottrell Reply Decl. ¶¶ 39-40; Swire Reply Decl. ¶ 68.

Dealers and other DMS providers alike agree that data integrators (and Authenticom in particular) do not harm DMS system integrity. *See* Fitkin Decl. ¶ 10; Whitworth Decl. ¶¶ 19-20. As Paul Whitworth of Cox – the third-largest DMS provider – makes clear, dealerships using Cox’s DMS may allow independent integrators to access the DMS, and those dealers do not suffer service disruptions or other harm to their DMS systems. *See id.*

Defendants fail to present any meaningful countervailing evidence. Defendants claim (at 11, 14) that “beginning in the early 2000s” third-parties’ actions “impair[ed] – and in some cases, even cripple[ed] – the DMS’s ability to function properly.” *See also* Defs. Opp. at 31-32. But they never say who these third-parties were or what they were doing, and provide no evidence that these decade-old incidents bear any resemblance to Authenticom’s operations. *See* Defs. SOAF ¶¶ 154, 197 (Dkt. 87); Thorne Decl. ¶ 40 (Dkt. 96); Schaefer Decl. ¶ 44 (Dkt. 97); Rosenbach Decl. ¶ 173 (Dkt. 129) (“Rosenbach Decl.”).

Defendants also assert (at 15-16) that “[h]ostile integrators’ activities posed significant burdens on [DMS].” *See also* Defs. Opp. at 32, 53. But CDK’s supporting declaration mentions

only the possibility that “Authenticom’s data access methods *can* place significant burdens on CDK’s systems and degrade system performance,” without identifying any burden Authenticom’s data access has *actually* imposed; nor does he explain how Authenticom’s access causes any such burden. Gardner Decl. ¶ 50 (Dkt. 93); *see also* Schaefer Decl. ¶ 46 (Dkt. 97) (similar statement from Reynolds’ executive). CDK complains that some of Authenticom’s queries could be more efficient but never says that the queries cause any DMS performance problems. *See* Gardner Decl. ¶ 53 (Dkt. 93). If Authenticom degraded system performance, one would expect Defendants’ Data Services executives – not to mention Defendants’ customers – to be able to identify actual examples. Indeed, except for a single isolated instance nearly a decade ago that was due to a stalled query, Defendants have never notified Authenticom of any possible degraded system performance. *See* Cottrell Reply Decl. ¶ 43.⁷

Defendants’ argument (at 2, 14, 32-33) that Authenticom may corrupt DMS data is likewise unpersuasive. Nearly all of Authenticom’s business, including its principal product (DealerVault), currently only “reads” from DMS; it does not “write” back to DMS and therefore cannot corrupt the data on the DMS. *See* Cottrell Reply Decl. ¶ 45. Moreover, where Authenticom provides “write” back services for dealers, it uses stringent quality control to ensure there are no errors in the data that is pushed back into the dealers’ DMS database. *See id.* ¶ 48. This service is highly reliable and generates only single digit errors – less than ten – out of tens of millions of records processed, which is an infinitesimal amount that is isolated to those individual records instead of affecting the DMS generally. *See id.* ¶¶ 47-49.

⁷ Defendants’ data security expert claims there was a single instance in which Authenticom’s software made 50,000 large data pulls from CDK in a single day. *See* Defs. Opp. at 33 (citing Rosenbach Decl. ¶ 174). Authenticom has been unable to confirm this event. But even if it did occur, this shows a possibility of degraded performance only in the rare case of a software glitch, not during Authenticom’s normal operations.

Defendants cite a review by CDK in August 2013 that identified numerous instances of data corruption. *See* Defs. Opp. at 14, 33 (citing Defs. Ex. 26 (Dkt. 106-33)). But that review stated that there were many sources of data corruption, including CDK's own 3PA program. *See* Defs. Ex. 26, at 2 (Dkt. 106-33). Even though the review singled out specific third parties (and CDK itself), it did not identify *Authenticom* as having caused any data corruption.⁸

b. Defendants Have No Evidence That Authenticom's Data Access Compromises Data Security

Defendants argue (at 53-56) that granting the preliminary injunction would pose data security risks or even expose the DMS to cyberattacks. Here again, however, Defendants offer virtually no evidence demonstrating that Authenticom's access has ever exposed Defendants' DMS systems to increased cybersecurity risk.

First, as Authenticom previously explained, and Defendants do not dispute, Authenticom has never had a data security breach in its 15-year history. *See* Mem. at 19 (Dkt. 61); Defs. RSOF ¶ 74 (Dkt. 86) ("Defs. RSOF"). Defendants' concerns are not even persuasive as a theoretical matter: Authenticom merely automates the process of extracting data from dealers' DMS systems using the same process dealers themselves would use if they each hired a crew of technicians to sit in front of a computer terminal to extract the data manually. Authenticom's processes are far more efficient – and thus procompetitive – but they do not fundamentally increase data security risks compared to the manual extraction of data.⁹

⁸ While Defendants state (at 33) that "[h]ostile integrators might also introduce unauthorized software to the system, or cause its computer code to be altered," Defendants present no evidence that Authenticom has ever done so – because Authenticom never has.

⁹ Defendants criticize (at 9, 31) Authenticom for requesting that dealers send account information to Authenticom via email. Defs. Ex. 61 (Dkt. 104-17), Defs. Ex. 63 (Dkt. 104-19). Authenticom's policy is that "login credentials should be sent to Authenticom via secure web form, and, if a dealer prefers to send login credentials via email, that the username and password

Second, Defendants’ own actions belie their sensationalized claims (at 53-55) of “intolerable” and “catastrophic” risks to “nearly a trillion dollars in commerce annually” and “tens of thousands of” jobs “if there were a massive cyberattack.” [REDACTED]

[REDACTED] Defendants also claim that they had supposed data security concerns as far back as 2000. Yet for all that time, until Defendants entered into their anticompetitive agreement in 2015, CDK touted its policy that it was “not going to limit the ability of a dealer to give an ID to someone else to, in essence, dial into their system. That is the dealer’s right. We have no right to tell them they can’t do that,” and openly supported data integrators like Authenticom. *See* SOF ¶¶ 44-45, 48-50, 54-55. To this day, CDK admittedly offers indistinguishable data integration services to dealers using other DMS systems. *See* Mem. at 7-8, 20; Defs. RSOF ¶¶ 31, 37. [REDACTED]

[REDACTED] And Reynolds agreed with its largest dealer customer (Penske Automotive Group) – whose preferences it could not afford to ignore – to allow Penske to use *Authenticom’s* data integration services. *See* Cottrell Reply Decl. ¶¶ 29-31. Likewise, Reynolds continues to use Authenticom to pull data from both Reynolds’ and CDK’s DMS customers for certain of

be sent to Authenticom in separate emails.” Cottrell Reply Decl. ¶¶ 20-23; *see* Swire Reply Decl. ¶ 52(c).

Reynolds' own applications. *Id.* ¶ 32. Defendants would have done none of these things if they had such grave security concerns.

Third, Defendants provide no supporting evidence from those who would suffer the harm from a data breach – the dealers.¹⁰ Data security breaches would damage dealers' customer relationships, and system integrity problems would harm their operations. Yet no dealer has submitted evidence supporting Defendants' claims, nor have Defendants disclosed any dealer that will provide such testimony. On the contrary, a dealer has averred these harms do not exist and is willing to so testify. *See* Fitkin Decl. ¶¶ 10-11. And, of course, if any dealer had any concerns that Authenticom created risks to security or system integrity, that dealer would not do business with Authenticom. *See* Defs. RSOF ¶ 36 ("Undisputed that dealer authorization is a necessary prerequisite to a data integrator pulling data.").¹¹

Fourth, Cox Automotive, the third largest DMS provider, confirms that CDK's and Reynolds' concerns are pretext. According to Cox Automotive, "data integrators such as Authenticom are typically able to access the dealership clients' data without creating unwarranted and unreasonable security risks." Whitworth Decl. ¶¶ 16-18. And renowned data security expert Peter Swire has opined that there is no security justification for Defendants'

¹⁰ Defendants claim (at 9, 54) that Authenticom has not formally agreed to warn dealers of data breaches. Authenticom, however, has agreed to "take commercially reasonable measures to protect Dealership Data," to hold that data "in strictest confidence," and to indemnify dealers for any security breach. *See* Pl. Ex. 28 at §§ 5.3, 6.3, 8.2, 9.1 (Dkt. 65-3) (DealerVault Terms & Conditions). Concomitant with those obligations, Authenticom would notify any dealer of a data breach as a matter of course.

¹¹ The only dealer declaration submitted by Defendants states that this particular dealer's employee is more "comfortable" using Reynolds' "Dynamic Reporting" feature than Authenticom's terminal emulation software because she prefers to be "manually involved" in exporting DMS data and feels that "Dynamic Reporting" gives her more "control [over] the data or data fields that are exported." Wood Decl. ¶¶ 6-7 (Dkt. 99).

blocking practices because, among other things, dealers control the data at issue and can share it as they please, data integrators are essential and well-accepted even in industries where far more sensitive data is at issue, and Authenticom has strong security practices. *See* Swire Decl. ¶¶ 7-27, 32 (Dkt. 58).¹²

Defendants suggest (at 12-14, 31) that two third-parties – the National Automobile Dealerships Association (“NADA”) and [REDACTED] – recommended that data integrators be blocked. They did not. NADA advised dealers to be vigilant about the data that third-parties access and to ensure that third-parties are bound by appropriate “contractual restrictions,” not that dealers sever relations with data integrators. Defs. Ex. 15, at 6 (Dkt. 106-15). Authenticom’s DealerVault is designed to comply with that guidance by allowing dealers to have complete control and visibility over the data that is accessed. *See* Mem. at 6; SOF ¶¶ 64-66, 68; Cottrell Reply Decl. ¶¶ 13, 38.¹³ Indeed, the President of the California New Car Dealers Association – the largest in the nation – will testify at the hearing that his association affirmatively recommends DealerVault to its dealers precisely because of the control DealerVault gives dealers over their data. *See* Maas Decl. ¶¶ 14-15. [REDACTED]

[REDACTED]

[REDACTED]

¹² Contrary to Defendants’ claim (at 8-9), Mr. Swire has reviewed Authenticom’s security practices and opined that they are strong. *See* Swire Decl. ¶ 32 (Dkt. 58); Swire Reply Decl. ¶¶ 39-52. Authenticom has also provided its Microsoft Application Development and Cloud Platform gold certifications with its reply papers. *See* Pls. Ex. 90. Those certificates require, among other things, that Authenticom pass rigorous exams. *See* Cottrell Reply Decl. ¶ 27.

¹³ Defendants note (at 31) that Authenticom may pull more data than any single vendor requires. Authenticom does so only with the permission of the dealer and only because, if Authenticom pulls all of the data required by a dealer’s many vendors, Authenticom needs to run only a single DMS query from which it delivers data to multiple vendors. This minimizes the number of queries on the DMS. *See* Cottrell Reply Decl. ¶ 38.

[REDACTED]

[REDACTED]

Fifth, contrary to Defendants’ claims (at 8, 14, 15, 33, 53-55) and consistent with Mr. Swire’s opinion, no sensitive information is at risk. While some sensitive information such as social security numbers, credit card information, or other proprietary information not belonging to the dealers may be stored in the DMS, Authenticom cannot access that sensitive information. *See* Cottrell Reply Decl. ¶¶ 15-18; Fitkin Reply Decl. ¶ 11; Whitworth Decl. ¶ 17. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Accordingly, Defendants reliance (at 13) upon data breaches concerning far more sensitive data are inapposite. *See* Swire Reply Decl. ¶¶ 27-35; *see also* Rosenbach Decl. ¶¶ 31, 46 (40 million credit card numbers and 80 million social security numbers stolen).¹⁴

In part for this reason, Defendants’ assertion (at 9, 54) that Authenticom has insufficient insurance in the event of a data breach is unsupported. Authenticom indemnifies dealers for “any data security event” caused by Authenticom up to \$20 million per occurrence. *See* Cottrell Decl. ¶ 32 (Dkt. 62); Pl. Ex. 28, § 9.1 (Dkt. 65-3) (DealerVault Terms & Conditions). There is no evidence that those policy limits are insufficient. Defendants cite the losses for the theft of 40 million credit card numbers from Target and 80 million social security numbers from Anthem, *see, e.g.*, Rosenbach Decl. ¶¶ 31-32, 46; they provide no evidence of what the losses might be

¹⁴ The data breach for the DealerBuilt DMS cited by Defendants (at 13 n.3) had nothing to do with data integrators. *See* Rosenbach Decl. ¶¶ 91-92.

for a data breach involving far less sensitive information of the far fewer customers of a car dealership. In any event, Authenticom has never had a data breach, let alone a reportable security incident. Cottrell Decl. ¶¶ 30, 32.

Finally, Defendants’ data security experts Eric Rosenbach’s and Paul Scheck’s opinions suffer from the same problems – non-existent and faulty evidence – as Defendants’ arguments. For example, Mr. Rosenbach’s opinion is premised on highly sensitive information such as social security numbers being accessible to Authenticom, but that is not correct, as Plaintiff’s data security expert, Peter Swire, explains. *See* Rosenbach Decl. ¶¶ 40-45, 158, 162; *see generally* Swire Reply Decl. (detailing the flaws in Mr. Rosenbach’s opinions). Mr. Schneck’s opinion is based on the mistaken premise that Authenticom interacts with a dealer’s DMS on a massive scale, whereas in reality the total data transmitted from a nightly batch download is approximately the same size as a single digital photo taken from a smart phone. *See generally id.* (detailing the flaws in Mr. Schneck’s opinion).

c. Claim of Harm To Investment Incentives Is Implausible And Unsubstantiated

Defendants argue (at 32, 34) that Authenticom is somehow “exploiting” their intellectual property and “parasitizing” their investment in the DMS platform, thereby dampening their “incentive to innovate.” But Authenticom does not depend on Defendants’ assistance to extract dealers’ data; it provides all the technology necessary to automate the extraction process and provide dealers and vendors with a streamlined, efficient way to use the data for critical software applications. Moreover, no one is asking CDK and Reynolds to give away their data integration products for free. Defendants can recover their investments in security and their data integration products by fairly competing in the market.

As to Defendants’ intellectual property argument, Defendants do not allege that Authenticom is violating any copyright or infringing any patent. And for good reason: Authenticom is not altering, copying, or downloading any of Defendants’ proprietary system – it is simply pulling data off a database, with the permission of the owner of the data (the dealer). Defendants’ argument that they have a proprietary right to prohibit such access is squarely foreclosed by the Seventh Circuit’s decision in *Assessment Technologies of Wisconsin, LLC v. WIREdata, Inc.*, 350 F.3d 640 (7th Cir. 2003). *WIREdata* is highly informative: the plaintiff in that case owned a database that stored a compilation of residential real-estate data that was collected and entered into the database by municipal property assessors. *Id.* at 647. The defendant, *WIREdata*, was in the business of extracting that data for use by real-estate brokers with the consent of the municipalities. The plaintiff tried to stop *WIREdata* from accessing its database, arguing that such access violated copyright law. The Seventh Circuit rejected that claim, holding that plaintiff had no right to stop the municipalities from obtaining their own information from the database, or from authorizing a third-party like *WIREdata* from doing so. Notably, the Court specifically commented that the municipalities could authorize “programmers furnished by *WIREdata* to use their computers to extract the data from their database.” *Id.* at 648. The Court also noted that the plaintiff’s attempt to prevent the municipalities “from revealing *their own* data . . . might constitute copyright misuse.” *Id.* at 646-47. So, too, here: Defendants, like the plaintiff in *WIREdata*, have no intellectual property right to prevent dealers from retrieve their own data from Defendants’ DMS, or to do that through Authenticom, the dealers’ agent; Defendants’ effort to exert proprietary control over the *data* that constitutes the lifeblood of the data integration market is an abuse of their monopoly power.

C. Granting Relief Is in the Public Interest

1. Absent an Injunction, Dealers, Vendors, and Car Buyers Will Suffer Higher Prices

The public interest, too, heavily favors entry of the preliminary injunction. Allowing Defendants to put Authenticom out business will inflict significant harm on the dealers and vendors that purchase Authenticom's services. The consequence of Authenticom's demise will be a further increase in Defendants' market power in the data integration market, with concomitant increases in prices. Defendants have already imposed dramatic price increases for those services since their unlawful 2015 agreement. *See, e.g.,* Singer Decl. ¶¶ 30-35, 44-48. These price increases also restrain competition in the software application market by impeding the development of new software applications by vendors – especially start-ups. Korp Decl. ¶¶ 14-17. If a preliminary injunction is denied, and Authenticom goes out of business, the impact on direct and indirect purchasers will be irreversible. *See Boardman v. Pacific Seafood Grp.*, 822 F.3d 1011, 1024 (9th Cir. 2016) (upholding a preliminary injunction where the public was at risk of suffering “substantially lessen[ed] competition”); *Collins Inkjet Corp. v. Eastman Kodak Co.*, 781 F.3d 264, 280 (6th Cir. 2015) (“The public interest is served by the injunction if the injunction is itself pro-competitive.”).

2. The Jobs and Livelihoods of Authenticom's Employees Further Support Preliminary Injunctive Relief

The interests of Authenticom's 120 employees also weigh heavily in favor of preliminary relief. If Authenticom fails, 120 Wisconsin employees will lose their jobs, and their families will suffer significant economic loss and displacement. Authenticom's 120 employees and the City of La Crosse – where Authenticom is among the largest employers and has led a downtown revitalization – will hardly be comforted by Defendants' glib response (at 55-56) that “it may

very well be that jobs would be gained elsewhere” if Authenticom’s workforce is displaced.¹⁵

Congressman Ron Kind, the City of La Crosse, and Wisconsin’s Economic Development Corporation are all behind Authenticom’s efforts to save itself and “level the playing field for Wisconsin’s small businesses.” *See* Pl. Exs. 100-101.

3. Authenticom’s Business Model Is Legal

Authenticom’s 15-year-old business does not violate the federal Computer Fraud and Abuse Act (“CFAA”) or Wisconsin’s state-law equivalent. The CFAA applies to persons who “intentionally accesses a computer *without authorization*” to obtain information from a protected computer. 18 U.S.C. § 1030(a)(2)(c) (emphasis added). Authenticom, by contrast, pulls dealers’ own data pursuant to dealers’ express authorization – all from the dealers’ own computer. Authenticom is standing in the shoes of an employee at the dealership and is therefore not “unauthorized” under the CFAA. *See, e.g., LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009) (“[A]n employer gives an employee ‘authorization’ to access a company computer when the employer gives the employee permission to use it.”); *see also International Airport Ctrs. LLC v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006) (analogizing from the law of agency to determine the scope of authorization). None of Defendants’ cited cases hold that “screen-scraping” violates the CFAA – which is not surprising given that it is a common practice

¹⁵ The public interest strongly favors “preserving a business that provides a valuable product to the community and preserving jobs.” *See, e.g., Stuller, Inc. v. Steak N Shake Enters., Inc.*, 2011 WL 2473330, at *13 (C.D. Ill. 2011); *Mem.* at 46-47 (citing cases). Defendants claim (at 46 n.11) that several of the cases Authenticom cited for this well-settled proposition were not antitrust cases, but that is beside the point: the public interest element of the preliminary injunction analysis applies regardless of the cause of action. And Defendants’ statement that non-antitrust cases do not account for “the possibility that jobs were being lost . . . due to vigorous and healthy competition” rings hollow, given that Defendants’ admitted and express aim is to eliminate the ability of dealers to choose Authenticom for the provision of data integration services.

across many industries, including in the banking and healthcare industries.¹⁶ See Swire Decl. ¶¶ 15-25.

D. The Injunction Sought Is Not a Mandatory Injunction And Satisfies Rule 65

Defendants describe (at 24) Authenticom’s requested relief as a “mandatory” injunction, arguing it should be subject to a higher legal standard. Often there is no sharp distinction between prohibitory and mandatory injunctions or between the standards governing the two. *Jacobson & Co. v. Armstrong Cork Co.*, 548 F.2d 438, 441 n.3 (2d Cir. 1977) (noting that prohibitory and mandatory injunctions are often “indistinguishable”). In this case, however, the relief being sought is prohibitory, not mandatory: Authenticom does not seek to compel Defendants to take any affirmative acts; it merely asks for an injunction requiring Defendants to refrain from blocking Authenticom’s dealer-authorized access to dealer data. See *Garcia v. Google, Inc.*, 786 F.3d 733, 740 (9th Cir. 2015) (en banc) (a mandatory injunction requires party “to take affirmative action”); *Stone v. City & Cty. of San Francisco*, 145 F.R.D. 553, 561 (N.D. Cal. 1993) (“prohibitory” injunction requires party to “refrain from doing a specified act”); *Legal Aid Soc’y of Haw. v. Legal Servs. Corp.*, 961 F. Supp. 1402, 1408 n.3 (D. Haw. 1997) (injunction prohibiting defendant from enforcing contractual restrictions is prohibitory, not mandatory).

Because Authenticom obtains authorization from *dealers*, Authenticom does not need and is not asking for Defendants’ assistance in accessing the DMS systems. Defendants suggest that they might have to take some affirmative technological actions even to discontinue blocking Authenticom. But any such steps cannot change the nature of Authenticom’s requested relief. A

¹⁶ See, e.g., *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581-82 (1st Cir. 2001) (liability turned on scope of defendant’s confidentiality agreement with plaintiff); *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178, 1182 (N.D. Cal. 2013) (liability turned on Craigslist’s ability to unilaterally “de-authorize” users from accessing its website).

landowner may need to take down a fence if enjoined from blocking a neighbor's enjoyment of an easement, but that does make the request a mandatory one. Otherwise, a party that has improperly impeded another's freedom to act – like the landowner in the prior example – could rely on its own improper conduct to impose a higher standard for injunctive relief. *See First Union Nat'l Bank v. Burke*, 48 F. Supp. 2d 132, 143 (D. Conn. 1999) (“[M]any prohibitory injunctions can easily be restated in a manner that makes them appear mandatory in effect.”).

Nor is there any merit to Defendants' suggestion (at 51-52) that the requested injunction is “impermissibly vague.” There is nothing complicated or unclear about an injunction against “[b]locking, disabling, or otherwise interfering with” Authenticom's dealer-authorized access to dealer data. Dealers have had a longstanding practice of permitting Authenticom to access their DMS systems through dealer-provided login credentials so that Authenticom can extract dealer data in an automated fashion on the dealers' behalf. CDK, in particular, not only permitted Authenticom to access dealer data stored on its DMS, but it also provided third-party data integration services to Reynolds' DMS customers for many years.¹⁷

¹⁷ A more explicit list of forbidden blocking activities is not required and would risk having “so much specificity as to create loopholes and opportunities for evasion.” *C & N Corp. v. Kane*, 142 F. Supp. 3d 783, 789 (E.D. Wis. 2015). Although the proposed preliminary injunction “does not choreograph every step, leap, turn, and bow” of the actions Defendants must refrain from taking, “it specifies the end results expected and allows the parties the flexibility to accomplish those results.” *North Alamo Water Supply Corp. v. City of San Juan, Tex.*, 90 F.3d 910, 917 (5th Cir. 1996) (per curiam); *see Russian Media Group, LLC v. Cable Am., Inc.*, 598 F.3d 302, 307 (7th Cir. 2010) (“[T]he injunction must also be broad enough to be effective, and the appropriate scope of the injunction is left to the district court's sound discretion.”).

II. AUTHENTICOM HAS SHOWN A STRONG LIKELIHOOD OF SUCCESS ON THE MERITS

Authenticom has shown a strong likelihood of prevailing on its antitrust claims because (1) the agreements between CDK and Reynolds to block Authenticom's access to their dealers' DMSs and to divide the market for integration services were unlawful *per se*; (2) their vertical agreements with dealers and vendors were unlawful as *per se* tying arrangements and under the Rule of Reason as unreasonable restraints; and (3) Authenticom has made a strong showing that each of the Defendants unlawfully monopolized an after-market for integration services. Given the strong showing of imminent harm and the lopsided balance of the equities, Authenticom's showing – strongly supported by the evidence even before discovery has begun – justifies relief. *Saad v. Village of Orland Park*, 2011 WL 6754042, at *1 (N.D. Ill. Dec. 23, 2011) (“The requirement that plaintiffs show some likelihood of success on the merits is a low threshold, requiring only that plaintiffs’ chances of prevailing be ‘better than negligible.’”) (quoting *Meridian Mut. Ins. Co. v. Meridian Ins. Grp.*, 128 F. 3d 1111, 1114 (7th Cir. 1997)).

A. Authenticom's Section 1 Claims Based on Horizontal Agreement Are Legally Unchallenged and Factually Supported

1. Defendants' Agreement To Block Authenticom Is Unlawful Per Se And Strongly Supported By the Evidence

Authenticom has shown that it is likely to succeed on its claim, under Section 1, that Defendants engaged in a *per se* unlawful conspiracy to exclude Authenticom (and other third-party integrators). Defendants do not and cannot claim that such an agreement could be justified by supposed concerns over data security and system integrity. Instead, Defendants insist that Authenticom's evidence of that agreement – including admissions by Defendants' own employees – should be disregarded, arguing that Defendants had little motivation to enter into such an agreement since they were capable of blocking Authenticom unilaterally. But

Defendants’ own evidence – including a clear statement in CDK’s own document that it intended to work with competitors to block independent integrators – and simple business logic strongly reinforce Plaintiffs’ claims.

First, although Defendants’ (mistakenly) quibble with the “group boycott” label, they do not and cannot argue that it would be anything but unlawful *per se* for horizontal competitors to agree to block a rival’s access to dealers’ data. As the Seventh Circuit has explained, “joint efforts by a firm or firms to disadvantage competitors by . . . persuading or coercing suppliers or customers to deny relationships the competitors need in the competitive struggle” are *per se* unlawful boycotts. *Toys “R” Us, Inc. v. FTC*, 221 F.3d 928, 936 (7th Cir. 2000). That is what occurred in this case: CDK and Reynolds agreed to block Authenticom from providing its competing integration service to their DMS customers.

Second, although Defendants generally claim that their conduct is justified by concerns over security and system integrity, they do not argue that such concerns are legally cognizable to justify a horizontal agreement as opposed to “independent decisions to ‘close’ their DMSs.” Defs. Opp. at 30. They are not. *See Klor’s, Inc. v. Broadway-Hale Stores, Inc.*, 359 U.S. 207, 212 (1959) (group boycotts “have not been saved by allegations that they were reasonable in the specific circumstances”). *National Soc’y of Prof’l Eng’rs v. United States*, 435 U.S. 679 (1978), is on point: there, petitioners – an association of engineers – argued that a horizontal restraint on price competition should be evaluated under the Rule of Reason, rather than being condemned as unlawful *per se*, because the restraint was allegedly justified by concerns about the “risk to public safety and health” from unregulated competition. *Id.* at 693. The Court rejected that argument, explaining that the Sherman Act’s “faith in the value of competition” precluded any inquiry into “whether competition is good or bad” in a particular instance. *Id.* at 695 (internal

quotation marks omitted). That principle precludes Defendants from defending their unlawful agreement on the ground that they shared mutual concerns about security.

Third, there is no reason for the Court to disregard the testimony of Authenticom CEO Steve Cottrell that two different executives at CDK and Reynolds told him they agreed to block third-party integrators, including Authenticom. Defendants' labeling of this evidence as "circumstantial" is inaccurate – the statement of a percipient witness that an agreement exists is direct, not circumstantial, evidence – and in any event does nothing to undermine the force of Mr. Cottrell's testimony. *See In re High Fructose Corn Syrup Antitrust Litig.*, 295 F.3d 651, 661 (7th Cir. 2002) (statements of defendants' employees direct evidence of antitrust conspiracy). A fact-finder could reasonably find the existence of an agreement based on that testimony alone, and the Court will have the opportunity to evaluate Mr. Cottrell's credibility for itself.

Fourth, the evidence revealed for the first time with Defendants' opposition confirms the existence of an unlawful horizontal agreement [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]. Even if such a commitment were not *per se* unlawful on its face, it renders incredible Defendants’ claim that they did not discuss – and share a mutual understanding about – a [REDACTED]

Fifth, the fact that both CDK and Reynolds abruptly changed their approach to third-party integration following the February 2015 agreement also supports the inference of agreement. For its part, CDK, which had always permitted third-party integrators to serve its DMS clients – successfully touting that as an advantage of its system over Reynolds’ – flipped, and began to block third-party integrators a few months after the agreement was signed. SOF ¶¶ 94, 96, 97, 100, 103, 104, 114. And Reynolds – which, as an application vendor, had previously made extensive use of Authenticom for access to CDK’s DMS clients, *see* Pl. Ex. 97 – also flipped, and began to switch to CDK’s integration service, which CDK agreed to provide *for free* for five years, Defs. Ex. 2, § 3(a) (Dkt. 106-2) (“No Fee Term”). The conclusion that Defendants were coordinating their approach to data integration is inescapable.

Sixth, the argument (at 28-29) that Defendants had no “economic incentive” to coordinate blocking of independent data integrators ignores evidence that when CDK competed by maintaining open access, Reynolds’ unilateral efforts to block third-party integrators were less profitable than concerted blocking would be. Before February 2015, according to Defendants’ expert [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

_____.

2. Defendants' Market Division Agreement Is Also Unlawful Per Se

[illegible]

18

19

[REDACTED]

[REDACTED]

Before this agreement, CDK and Reynolds competed to provide data integration services for car dealerships that use the Reynolds DMS platform. After the agreement, CDK agreed to shutter that business and steer its existing customers to Reynolds. The agreement replaced competition with cooperation. Even without more – and there is much more – such an agreement constitutes illegal market allocation. *See General Leaseways, Inc. v. National Truck Leasing Ass’n*, 744 F.2d 588, 595 (7th Cir. 1984) (affirming grant of preliminary injunction because “the division of markets . . . is a per se violation of section 1 of the Sherman Act.”); *see also* Singer Reply Decl. ¶¶ 2-3.

Defendants assert (at 26) that “it is implausible” that “sophisticated business entities represented by experienced in-house and outside counsel . . . would commit a *per se* violation of the Sherman Act by reducing it to a lengthy written agreement.” [REDACTED]

[REDACTED]

[REDACTED] Defendants recognized that they were on thin antitrust ice, or they would not have included a written disclaimer. And it is hardly unprecedented that written agreements, even those signed by large and sophisticated corporations, can violate the antitrust laws. *See, e.g., United States v. Apple, Inc.*, 791 F.3d 290, 320 (2d Cir. 2015) (*per se* conspiracy between Apple and book publishers based in part on written contract terms); *United States v. Mercedes-Benz of N. Am., Inc.*, 517 F. Supp. 1369, 1374 (N.D. Cal. 1981) (same).

Defendants’ characterization (at 27) of their February 2015 agreement as a “settlement” to discontinue CDK’s purportedly “hostile” data integration services does not change the

analysis. Whatever Defendants call it, the February 2015 agreement is not immune from the antitrust laws. *See Premier Elec. Constr. Co. v. National Elec. Contractors Ass’n, Inc.*, 814 F.2d 358, 376 (7th Cir. 1987) (“[w]hen private parties help themselves to a reduction in competition, the antitrust laws apply”); *Andrx Pharm., Inc. v. Biovail Corp. Int’l*, 256 F.3d 799, 818–19 (D.C. Cir. 2001) (private settlement not immune from antitrust laws); *American Needle, Inc. v. National Football League*, 560 U.S. 183, 193 (2010) (“The Sherman Act ... is aimed at substance rather than form.”).

B. Authenticom Is Likely To Succeed on Its Tying Claim

Defendants do not contest that (1) each of them provides DMS service (the tying product) to its clients only on the condition that their clients also agree to use only its DMS provider’s integration services (the tied product); (2) each of them has sufficient economic power in the DMS market to restrain free competition in integration services; and (3) each of the arrangements at issue affects a substantial volume of interstate commerce. These facts suffice to establish that each of the Defendants has engaged in tying that is unlawful *per se* under Section 1. *See* Mem. at 33-36.

Defendants cannot escape liability by arguing that vendors, rather than dealers, directly pay for integration services. They cite no case to support such a loophole. On the contrary, it is uncontested that *dealers* – not vendors – make the decision about which integrators will be permitted access to their system, *see* SOF ¶¶ 36-39; dealers are therefore the relevant target of Defendants’ tying arrangement. It does not matter that vendors pay the integration service fees; the dealers still control the selection of integration services, which is what matters for purposes of a tying claim. *See Dos Santos v. Columbus-Cuneo-Cabrini Med. Ctr.*, 684 F.2d 1346, 1354 (7th Cir. 1982) (hospital, rather than patient, may be relevant purchaser for antitrust purposes

because the “patient generally takes no part in the selection of a particular anesthesiologist,” even though the hospital may bear none of the costs). And that conclusion gains added force from the fact that the dealers ultimately bear the cost of integration services indirectly through the cost of the applications they purchase from vendors. *See, e.g.*, Korp Decl. ¶¶ 27, 29 (Dkt. 54); *see also* Defs. RSOF ¶ 253 (Defendants acknowledging that “some vendors pass through some” or “all” of “their integration fees”).

Defendants’ argument that they are permitted to introduce pro-competitive justifications in defense of such a per se unlawful tying arrangement is incorrect. *See Jefferson Par. Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 16 (1984), *abrogated on other grounds by Illinois Tool Works Inc. v. Independent Ink, Inc.*, 547 U.S. 28 (2006) (Once the plaintiff shows the three required elements for a tying claim, “*per se* prohibition [of tying] is appropriate if anticompetitive forcing is likely.”); *Gumwood HP Shopping Partners, L.P. v. Simon Prop. Grp., Inc.*, 2016 WL 6091244, at *11 (N.D. Ind. Oct. 19, 2016) (“The law prescribes certain elements that may be proven to establish that a tying arrangement is unlawful under the per se tying framework If a plaintiff proves those elements, then the conduct is deemed anticompetitive.”).²⁰ In any event, taken at face value, Defendants’ arguments would only mean that their agreements with dealers are subject to scrutiny under the Rule of Reason, not that they are lawful. As discussed below, Defendants’ vertical agreements are unlawful under that standard as well.

²⁰ *Batson v. Live Nation Entm’t, Inc.*, 746 F.3d 827 (7th Cir. 2014) is not to the contrary – that case did not involve an antitrust tying claim at all, and the Court expressly recognized that tying arrangements violate Section 1 of the Sherman Act “if the seller has appreciable economic power in the tying product market and if the arrangement affects a substantial volume of commerce in the tied market.” *Id.* at 832 (internal quotation marks omitted). As noted in text, there is no dispute that those requirements are satisfied in this case.

C. Authenticom Is Likely To Succeed on Its Claims Under the Rule of Reason

The mutually reinforcing restraints that each of the Defendants imposes on dealers and vendors violate Section 1 of the Sherman Act because they unreasonably restrain competition without any legitimate pro-competitive justifications.

Defendants do not dispute that each of the Defendant's agreements with its dealers and the vendors who provide service to them foreclose a substantial amount of competition. *See* Mem. at 28-30. Nor do Defendants seriously dispute that these agreements have led to massive increases in the prices for integration services. *See id.* 30-31. Defendants' expert does not dispute the accuracy of the price increase that Dr. Singer reported. And while he asserts that Dr. Singer failed to account for the "quality-adjusted" price of the integration services that Defendants provide, he has no evidence – despite access to the Defendants' business information – that those services offer *any* quality advantage over the services that Authenticom provides, let alone one that would justify the massive price increase in prices that vendors have experienced. *See also* Singer Reply Decl. ¶¶ 7-12.

Defendants' argument (at 44) that they do not engage in textbook "exclusive dealing" is beside the point, because Section 1 reaches all unreasonable agreements in restraint of trade. *See Arizona v. Maricopa Cty. Med. Soc'y*, 457 U.S. 332, 343 (1982). Moreover, Defendants' argument on this score is squarely contrary to the evidence: they insist that their arrangements with vendors are not exclusive dealing arrangements because "3PA [CDK's data integration product] and RCI [Reynold's data integration product] are not competing data integrators." Defs. Opp. at 44. But that is not so: the parties' own documents make clear that they provide integration services in competition with "hostile integrators" like Authenticom. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Defs. Ex. 17 at 9 (CDK’s 2015 10-K identifying CDK’s “Data Management & Business Intelligence Solutions” as a separate “Solution” that “may be implemented as a stand-alone product or solution without the core Dealer Management System”).

2. Defendants’ argument that the restraints at issue are justified by concerns over “security” and “system integrity” is contrary to the evidence, which makes clear that the restraints at issue are designed to exploit, not protect, dealers and vendors. As explained at length above, *see supra* pp. 10-18, there is no evidence that Authenticom has ever caused a security breach or has ever been associated with any negative impact on DMS performance. If there were such evidence, Defendants would have every incentive to provide it.

Defendants’ own documents make clear that the motivation behind CDK’s switch to a closed system was [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]. *Id.* at 16. Based on the evidence, there is every likelihood that a fact-finder would conclude that Defendants’ security justifications are pretextual.

3. Even if Defendants security and system integrity concerns were valid, they still would not justify the measures that Defendants have taken to block independent integrators’ ability to provide service to dealers and vendors. The use of third-party data integrators is standard practice in many industries. *See Swire Decl.* ¶¶ 15-25. Defendants offer no reason that the same measures that protect sensitive personal information in the health care industry would

be insufficient to protect much less sensitive commercial information in the automotive industry. Given the massive price increase that Defendants' policies have caused and the absence of any justification for the restrictions they have imposed, Defendants' agreements unreasonably restrain trade and violate Section 1. *See American Bar Association, Antitrust Law Developments* 80 (7th ed. 2012) ("a restraint with a net effect of increasing price . . . would probably fail the balancing test").

D. Authenticom Is Likely To Succeed On Its Section 2 After-Market Claims

Authenticom is also likely to succeed on its Section 2 monopolization claim. Defendants have market power in the after-market for integration services provided to their own dealers and have acquired and maintained that power through a variety of anticompetitive contractual restraints and tactics. Defendants offer no persuasive reason to ignore the existence of these discrete economic markets or to ignore the evidence that they maintain their monopoly power through unlawful exclusionary conduct.

1. Authenticom has provided strong evidence that Reynolds and CDK each provide integration services to their dealers in a separate after-market: most obviously, CDK and Reynolds have excluded competition and raised data integration prices above competitive levels on their platforms. That is quintessential market power. *Gumwood HP Shopping Partners*, 2016 WL 6091244, at *7 ("[A] firm is a monopolist if it can profitably raise prices substantially above the competitive level . . . [W]here evidence indicates that a firm has in fact profitably done so, the existence of monopoly power is clear." (quoting *United States v. Microsoft Corp.*, 253 F.3d 34, 51 (D.C. Cir. 2001)); *SanDisk Corp. v. Kingston Tech. Co.*, 863 F. Supp. 2d 815, 824 (W.D. Wis. 2012) ("Market power may be . . . shown by direct evidence of anticompetitive effects on price or output.")).

Nevertheless, Defendants claim that there is adequate competition in the market for DMSs to constrain Defendants' ability to charge supracompetitive prices for integration services.²¹ But this is precisely the argument that the Supreme Court rejected in *Eastman Kodak Co. v. Image Technical Services*, 504 U.S. 451, 482 (1992). Defendants point to evidence (at 36-37) that [REDACTED] of DMS customers are up for renewal in any given year and, within that subset, [REDACTED] switched providers in 2016. But that hardly proves Defendants' case: on the contrary, by Defendants' own calculation, the incumbent provider remains in place for nearly [REDACTED] of the market in any given year – [REDACTED] – in a market where the average DMS tenure is over 20 years. “Market definition is an intensely factual determination and proper market definition can be determined only after a factual inquiry into the ‘commercial realities’ faced by consumers.” *Morton Grove Pharm., Inc. v. Par Pharm. Cos.*, 2006 WL 850873, at *9 (N.D. Ill. Mar. 28, 2006) (citing *Eastman Kodak*). A jury could reasonably find that, in those market conditions, Defendants “profitably could maintain supra-competitive prices in the aftermarket,” *Eastman Kodak*, 504 U.S. at 476 – especially in light of the un rebutted pricing evidence showing that Defendants have done just that. *See also Red Lion Med. Safety, Inc. v. Ohmeda, Inc.*, 63 F. Supp. 2d 1218, 1232 (E.D. Cal. 1999) (holding that where there is

²¹ Defendants' claims (at 37) of “robust competition” in the DMS market are vastly overstated. CDK and Reynolds are longstanding DMS duopolists. Defendants control 72 percent of the market – and an even larger share if measured by car sales rather than dealership rooftops. *See* Defs. RSOF ¶ 7 (“Undisputed that CDK's and Reynolds' respective market presence may be larger if measured by the number of vehicles sold by their dealer customers.”). And, Defendants hardly “compete vigorously” (at 37) for the sliver of dealerships that are up for grabs in any given year. On the contrary, since the February 2015 agreement, Defendants are in lockstep and no longer compete at all on the basis of what was formerly a key point of differentiation between them – third-party access to their systems. *See Datel Holdings Ltd. v. Microsoft Corp.*, 712 F. Supp. 2d 974, 988-89 (N.D. Cal. 2010) (*Eastman Kodak* claim particularly strong where the primary market featured two dominant players and was “also not very competitive.”).

competing evidence on the degree of lock-in, “these are disputed issues for trial” that cannot be resolved on summary judgment).

2. The evidence also contradicts Defendants’ claim (at 37-38) that consumers were not victimized by any change in policy because their DMS contracts have long had provisions prohibiting “unauthorized access.” At the outset, far from prohibiting third-party access, [REDACTED]

[REDACTED] In any event, whatever the contracts say or mean, there is no dispute that Defendants’ *policies* with regard to third-party integration services sharply changed.

[REDACTED] Yet until recently, CDK repeatedly and publicly supported independent data integration and provided such dealer-authorized integration services itself, including on the Reynolds system. CDK’s own CEO, with respect to dealers’ use of independent integrators like Authenticom, publicly stated: “We’re not going to prohibit that or get in the way of that. I don’t know how you can ever make the opinion that the data is yours to govern and to preclude others from having access to it, when in fact it’s really the data belonging to the dealer. As long as they grant permission, how would you ever go against that wish?” Pl. Ex. 19. And yet, after entering the agreement with Reynolds, CDK did “go against that wish.” Reynolds, too, admits that it changed its policy with regard to enforcement of its DMS agreements – with tepid blocking in 2009, followed by more aggressive blocking since 2013. With the average DMS client tenure exceeding 20 years, most dealers were “locked in” long before recent changes in policy. And Defendants’ own cases recognize that a company’s “change in policy” is a “crucial factor” in the *Eastman Kodak* analysis. *PSI Repair Servs., Inc. v. Honeywell, Inc.*, 104 F.3d 811, 820 (6th Cir.

1997) (“By changing its policy after its customers were ‘locked in,’ Kodak took advantage of the fact that its customers lacked the information to anticipate this change.”).

Furthermore, there are additional “information costs,” *Eastman Kodak*, 504 U.S. at 474, that impede switching between DMS brands in response to an increase in the price of integration services. Vendors, not dealers, directly incur those charges, and Defendants impose price secrecy provisions that prevent vendors from telling dealers the source of integration-related price increases. SOF ¶¶ 166-69. The point of these provisions is ensure that there is a “less responsive connection between,” *Eastman Kodak*, 504 U.S. at 474, supracompetitive prices in the data integration aftermarket and competition in the DMS market, *see* [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Consistent with this analysis, courts have recognized *Eastman Kodak* claims notwithstanding an “unauthorized access” provision in the initial contract. In *Datel Holdings*, for example, the initial contract gave the manufacturer (Microsoft) the right to prohibit “unauthorized” accessories and hardware on its Xbox game system. 712 F. Supp. at 988-90. The court rejected Microsoft’s attempt to dismiss the *Eastman Kodak* claim on this basis, because it was a factual question as to whether a “customer purchasing an Xbox 360 console would understand the contract as prohibiting unauthorized accessories.” *Id.* at 989; *see also Burda v. Wendy’s Int’l, Inc.*, 659 F.Supp.2d 928, 935 (S.D. Ohio 2009) (*Eastman Kodak* claim cognizable despite “authorized supplier” provision in initial franchise agreement); *Avaya Inc. v. Telecom Labs, Inc.*, 2014 WL 2940455, at *6 (D. N.J. June 30, 2014) (jury found for plaintiff on *Eastman*

Kodak claim based on contract-based ban of “unauthorized” service providers for Avaya-brand phones).

3. Defendants argue (at 40) that they did not acquire or maintain their monopoly through exclusionary conduct. But the same conduct that supports Authenticom’s claims under Section 1 supports its Section 2 claims *a fortiori*. See, e.g., *ZF Meritor, LLC v. Eaton Corp.*, 696 F.3d 254, 271 (3d Cir. 2012) (“Exclusive dealing arrangements are of special concern when imposed by a monopolist.”); *Gumwood HP Shopping Partners, L.P. v. Simon Prop. Grp., Inc.*, No. 3:11-CV-268 JD, 2013 WL 3214983, at *7 (N.D. Ind. Mar. 13, 2013) (“Where defendant has engaged in unlawful restraint of trade that would independently violate Section 1 of the Sherman Antitrust Act, it is well established that it also violates Section 2 if it acquires or maintains a monopoly by means of that restraint of trade.”). Defendants ignore this conduct.

Verizon Commc’ns Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398 (2004), does not support Defendants because Authenticom is not seeking Defendants’ *cooperation* or a regime of “forced sharing.” See *id.* at 408. Rather, Authenticom wants Defendants to stop blocking dealers and vendors from doing business with Authenticom by using the system’s existing capabilities. Authenticom is not free-riding on anyone’s investment any more than TurboTax or Mint “free ride” on banking systems when they screen-scrape financial information to automate tax-preparation and financial-planning services. Authenticom provides a service to dealers – using the same report-generating functions that are already available to dealers – on the dealers’ behalf.

E. Because the Restrictions on Dealing with Independent Integrators Are Unlawful, Defendants’ Conduct Is Not Privileged, and Authenticom’s Tortious Interference Claim Is Likely To Succeed

Defendants cannot meet their burden of proving that their intentional interference with Authenticom’s contracts is justified. *See Briesemeister v. Lehner*, 720 N.W.2d 531, 543 (Wis. Ct. App. 2006). Conduct that violates the antitrust laws cannot justify interference with contracts. *See* Restatement (Second) of Torts § 767 cmt. c. Independent of that, none of the justifications advanced by Defendants is likely to succeed.

First, Defendants’ alleged security concerns are drastically overstated in light of Authenticom’s unblemished security record and the fact that other DMS providers allow independent integration, as did CDK itself until two years ago. *Second*, Defendants assert that the “nature” of their conduct justifies their interference because they did not use “direct threats, coercion, or economic pressure toward Authenticom.” Defs. Opp. at 46. But the evidence shows that Defendants directly threatened Authenticom, dealers, and vendors, *see* Cottrell Decl. ¶¶ 48-53 (Dkt. 62), and spread disparaging and false information about Authenticom’s security to its customers. *See* SOF ¶¶ 213-30. Finally, Defendants’ conduct does not fall within the “Asserting a Bona Fide Claim” exception to tortious interference. *See* Restatement (Second) of Torts § 733. This exception is “narrow in scope” and only applies where the defendant pursues its interest through the *legal process* – not where, as here, Defendants engaged in self-help designed to destroy Authenticom’s business relationships. *See Briesemeister*, 720 N.W.2d at 544.

III. NO BOND IS WARRANTED

The Court should not require Authenticom to post a security bond under Rule 65(c); if any bond is required, it should be modest in light of the extensive damage Defendants have already done to Authenticom’s financial health. District courts have broad discretion to waive

Rule 65(c)'s injunction bond. *See Wayne Chem., Inc. v. Columbus Agency Serv. Corp.*, 567 F.2d 692, 701 (7th Cir. 1977) ("Under appropriate circumstances bond may be excused, notwithstanding the literal language of Rule 65(c)."). Waiver of the bond requirement is appropriate in this case for three reasons.

First, it is appropriate to "waive the requirement of an injunction bond when the court is satisfied that there's no danger that the opposing party will incur any damages from the injunction." *Gutierrez v. City of East Chicago*, 2016 WL 5819818, at *13 (N.D. Ind. Sept. 6, 2016). Defendants bear the burden of showing that the entry of a preliminary injunction will cause them concrete harm. *See Monster Energy Co. v. Wensheng*, 136 F. Supp. 3d 897, 911 (N.D. Ill. 2015). Here, Defendants have not carried that burden. As explained above, Defendants' claims of harm are purely speculative and inconsistent with the evidentiary record. Authenticom has been engaged in third-party access of Defendants' systems for years, yet Defendants cannot point to a single concrete instance where they have suffered economic damage. Defendants' competitor, Cox, has permitted third-party access for years, without incident. In particular, Reynolds' assertion (at 57) that it would need to spend *hundreds of millions of dollars* "to redesign core components of its systems" is not credible.

Second, courts appropriately waive the bond requirement when the injunction sought is in the public interest. *See Concerned Pastors for Social Action v. Khouri*, 220 F. Supp. 3d 823, 829 (E.D. Mich. 2016) ("[T]he Court has significant discretion to waive the bond requirement in light of the public interest."). *Carrillo v. Schneider Logistics, Inc.*, 823 F. Supp. 2d 1040, 1047 (C.D. Cal. 2011). As described above, a preliminary injunction would prevent Defendants from extinguishing their only remaining competitor in the data integration market, and would prevent dealers and vendors from having to pay significantly higher prices. Because Authenticom's

lawsuit directly benefits the public interest, *see supra* at 24-25, the bond requirement should be waived.

Third, courts have recognized that waiver of the bond requirement is appropriate where the plaintiff lacks the financial resources to post security. Here, requiring Authenticom to post a significant bond, as Defendants request, would undermine a principal objective of preliminary injunctive relief – namely, to keep Authenticom from going out of business before it can vindicate its claims through this litigation. *See Navajo Health Found.-Sage Mem'l Hosp., Inc. v. Burwell*, 100 F. Supp. 3d 1122, 1191-92 (D. N.M. 2015) (“Forcing [plaintiff] to post such a large bond risks defeating this preliminary injunction’s purpose: keeping [plaintiff] afloat until this case’s resolution.”); *accord Carrillo*, 823 F. Supp. 2d at 1047.

In all events, Defendants’ demand for a \$10 million bond is grossly inflated. If the Court determines that some bond is appropriate, it should set that bond at no more than \$1 million, in light of (1) the lack of evidence of any realistic danger of serious economic harm to Defendants; (2) the fact that Defendants’ conduct has already seriously weakened Authenticom’s ability to post security; (3) Authenticom’s existing \$20 million cybersecurity insurance policy in the unprecedented event of a data breach implicating Authenticom’s services; and (4) Authenticom’s strong likelihood of success on the merits. *See, e.g., In re Washington State Apple Advert. Comm’n*, 257 F. Supp. 2d 1274, 1289 (E.D. Wash. 2003).

CONCLUSION

The Court should grant Authenticom’s Motion for a Preliminary Injunction.

Dated: June 22, 2017

Respectfully submitted,

s/ Jennifer L. Gregor

Jennifer L. Gregor
Mark W. Hancock
GODFREY & KAHN, S.C.
One East Main Street, Suite 500
Madison, WI 53703
Phone: 608-257-3911
Fax: 608-257-0609
Email: jgregor@gklaw.com,
mhancock@gklaw.com

Michael N. Nemelka (*pro hac vice*)
Aaron M. Panner (*pro hac vice*)
David L. Schwarz (*pro hac vice*)
Kevin J. Miller (*pro hac vice*)
Derek T. Ho (*pro hac vice*)
Joshua Hafenbrack (*pro hac vice*)
Joanna T. Zhang (*pro hac vice*)
KELLOGG, HANSEN, TODD, FIGEL &
FREDERICK, P.L.L.C.
1615 M Street, N.W., Suite 400
Washington, D.C. 20036
Phone: (202) 326-7900
Fax: (202) 326-7999
Email: mnemelka@kellogghansen.com
apanner@kellogghansen.com
dschwarz@kellogghansen.com
kmiller@kellogghansen.com
dho@kellogghansen.com
jhafenbrack@kellogghansen.com
jzhang@kellogghansen.com

Attorneys for Plaintiff Authenticom, Inc.